



1/10

100

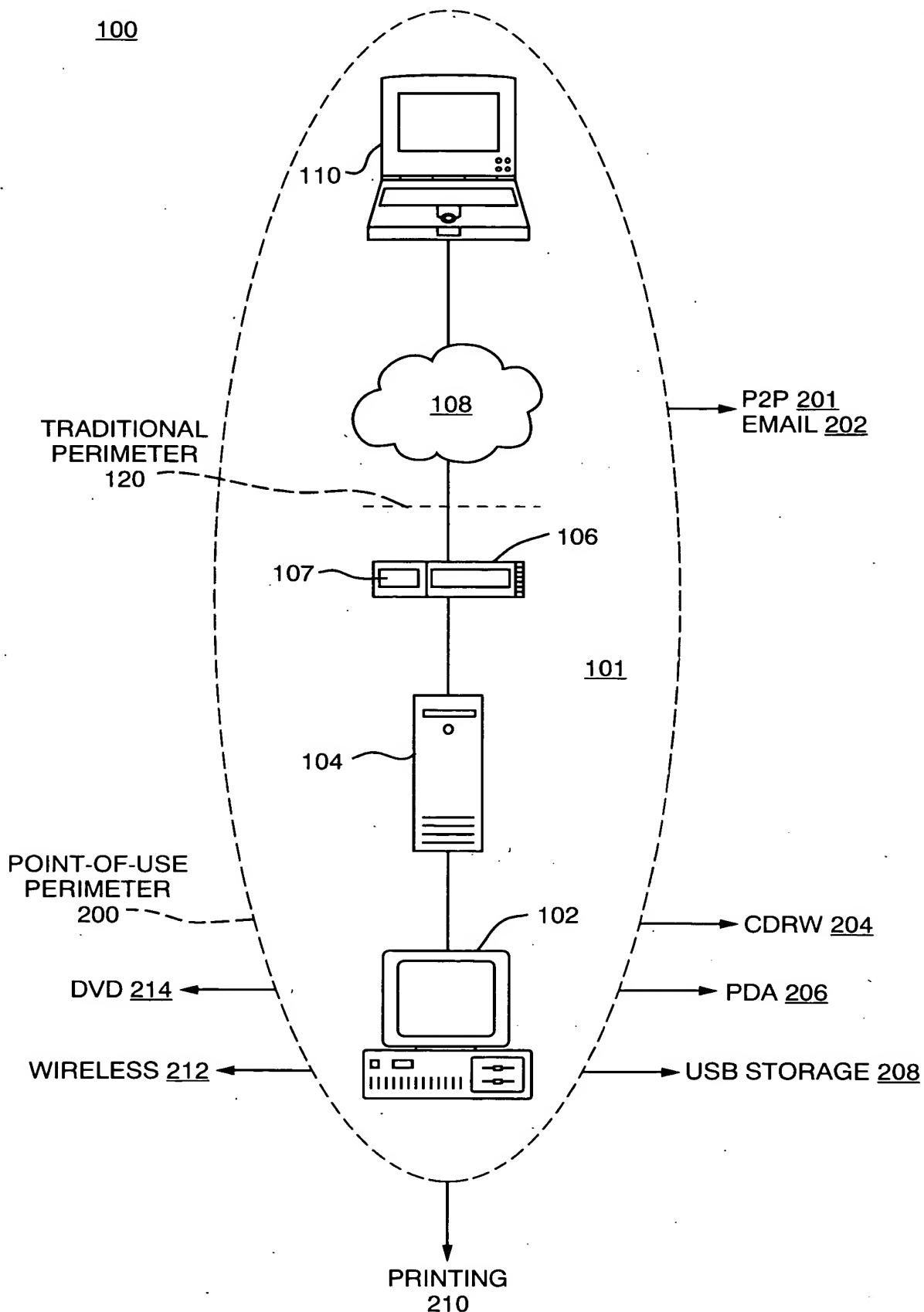


FIG. 1

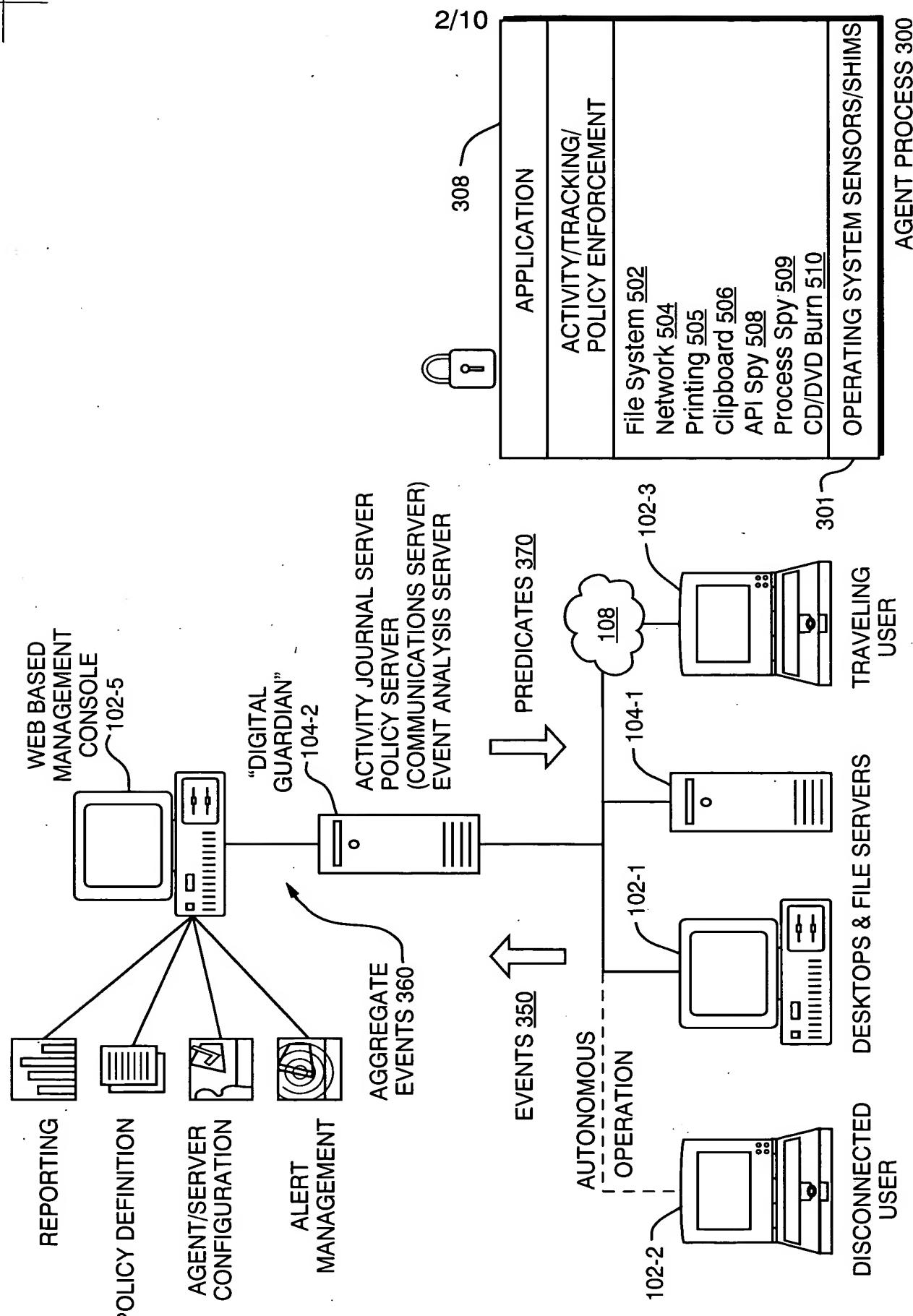


FIG. 2

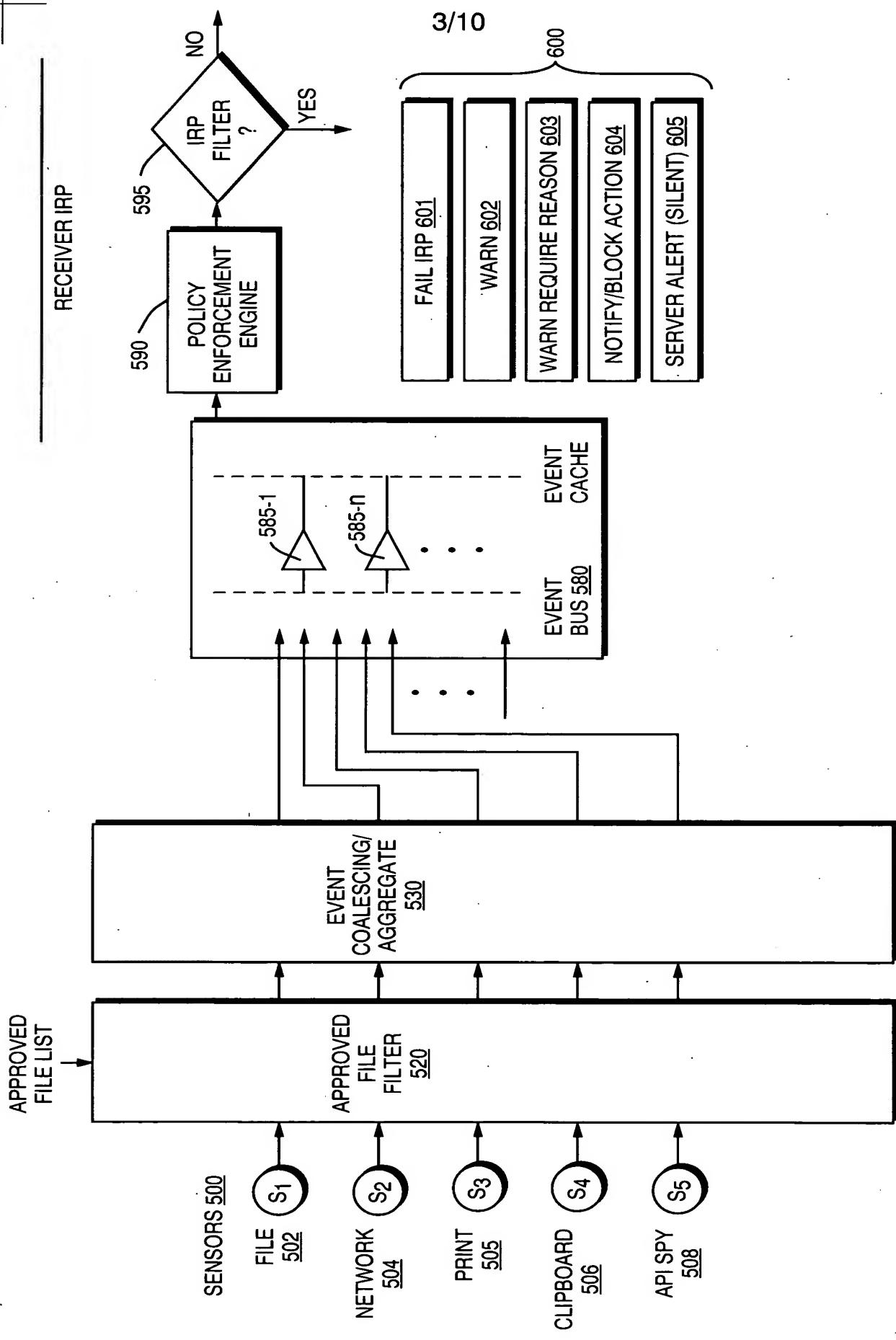


FIG. 3

Action Type	Level	Event Category	Event Name	Event Table	Action Detail Field	Action Detail Value	Discriminant
1	Low	File	FileRead	FileEvent	operationType	0	bytesRead > 0, bytesWritten = 0
2	Low	File	FileWrite	FileEvent	operationType	0	bytesRead = 0, bytesWritten > 0
3	Low	File	FileReadWrite	FileEvent	operationType	0	bytesRead > 0, bytesWritten > 0
4	Low	File	FileCopy	FileEvent	operationType	1	
5	Low	File	FileRename	FileEvent	operationType	2	
6	Low	File	FileDelete	FileEvent	operationType	3	
7	Low	File	FileMove	FileEvent	operationType	4	
8	Low	File	FileRecycle	FileEvent	operationType	5	
9	Low	File	FileRestore	FileEvent	operationType	6	
10	Low	Network	TCPPIInbound	NetworkEvent	protocolType	TCPIP	isOutbound = 0
11	Low	Network	TCPPIOutbound	NetworkEvent	protocolType	TCPIP	isOutbound = 1
12	Low	Network	UDPIInbound	NetworkEvent	protocolType	UDP	isOutbound = 0
13	Low	Network	UDPOutbound	NetworkEvent	protocolType	UDP	isOutbound = 1
14	Low	Network	IPSECInbound	NetworkEvent	protocolType	IPSEC	isOutbound = 0
15	Low	Network	IPSECOutbound	NetworkEvent	protocolType	IPSEC	isOutbound = 1
16	Low	Print	PrintEvent	(implied)		N/A	
17	Low	CD	CDRead	CDEvent	operationType	1	
18	Low	CD	CDWrite	CDEvent	operationType	2	
19	Low	Clipboard	ClipboardCutCopy	ClipboardEvent	eventType	CutCopy	
20	Low	Clipboard	ClipboardPaste	ClipboardEvent	eventType	Paste	
21	Low	User	UserLogon	UserEvent	eventType	Logon	
22	Low	User	UserLogout	UserEvent	eventType	Logoff	
23	Low	Machine	Machine	MachineEvent	eventType	...	Skip the Machine events

FIG. 4A

			ProcessStart ProcessEnd	Process Process	(Implied) (Implied)		Use processStartDtTm Use processEndDtTime
24	Low	Process					
25	Low	Process					
26	High	File	FileEdited		AggregateEvent		
27	High	File	FileCopied		AggregateEvent		
28	High	File	FileSaveAs		AggregateEvent		
29	High	File	FileLeftThroughRemovableMedia		AggregateEvent		
30	High	Clipboard	ClipboardToFile		AggregateEvent		
31	High	Print	PrintFile		AggregateEvent		
32	High	CD	BurnMaster		AggregateEvent		
33	High	CD	BurnFile		AggregateEvent		
34	High	Network	FileLeftThroughNetworkPort		AggregateEvent		
35	High	Network	EmailFile		AggregateEvent		
36	High	Network	RemoteAccess		AggregateEvent		
37	High	Network	InstantMessenger		AggregateEvent		
38	High	Network	P2PApp		AggregateEvent		
39	High	Network	FTPFile		AggregateEvent		
40	High	Network	TunnelOut		AggregateEvent		
41	High	Network	TunnelIn		AggregateEvent		
42	High	Network	TunnelInOut		AggregateEvent		
43	High	Network	FileOutThroughTunnel		AggregateEvent		

FIG. 4B

6/10

Event Name	Constituent Event Types	Pattern	Scope
FileEdited	FileRead, FileWrite, FileReadWrite	Same processid and fileHandle. beforeHash of first read & afterHash of last write differ. Both reads and writes to same fileHandle. Sum of writes > 0.	Thread
FileCopied	FileRead, FileWrite, FileReadWrite, FileCopy	Command shell: Alternating reads & writes. The reads all have one fileHandle, the writes all have a second one. Explorer: A long series of reads from one fileHandle followed by a long series of writes to a second. Mind the time period between. In both cases, the target device must not be removable.	Thread
FileSaveAs	FileRead, FileWrite, FileReadWrite	An app reads one or more files then writes a file.	Process
FileLeftThroughRemovableMedia	FileRead, FileWrite, FileReadWrite, FileCopy	Same as FileCopied or FileSaveAs, but target device is removable.	Process
ClipboardToFile	ClipboardCutCopy, ClipboardPaste	Pair a ClipboardCutCopy with all subsequent Clipboard Paste events for that user login until the next copy or the user logs out. Problem: If the user closes the application that performed the copy and the object was large and the user opts not to keep it there, what happens?	Login

FIG. 5A

PrintFile	Print, possibly others	Unclear. If there are temp files, intermediate PDF files, etc. then we may perform a chain of custody analysis to figure out just what was printed.	Thread
BurnMaster	FileRead, FileWrite	An app known to burn files reads one or more files then writes a file.	Process
BurnFile	CDWrite, FileRead	Application is recognized as a CD writing app. (Optional) Series of FileReads from one fileHandle, followed by a series of CDWrite events with the same process. May need to compare filenames, otherwise one read will exhaust all the writes. Alternately, all read files are lumped together with one large burn event. Or perhaps the first read of a new file after the last read from the previous file is the start of the next burn event.	Process
FileLeftThroughNetworkPort		An overlapping stream of FileReads interspersed with Inbound and Outbound network events. All the network events should be for the same port (?) and to a destination NOT on localhost.	Thread
EMailFile		All the network events should be for the same protocol. Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be an email program. May place constraints on the ports, since many emailers use certain well defined ports for SMTP, POP, etc.	Process

FIG. 5B

InstantMessenger	FileRead, TCPPIInbound, TCPIPOutbound, (other protocols???)	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be used for instant Messenger.	May place constraints on the ports.	Process
P2PApp	FileRead, TCPPIInbound, TCPIPOutbound, UDPIPInbound, UDPPOutbound, IPSECIInbound, IPSECOutbound	Constrain the application name to be one of those known to be a P2PApp. Multiple ports will be used; some or all of them may have constraints. May constrain the protocol per app or per instance.	Similar to FileLeftThroughNetworkPort as concerns interleaved file reads.	Process
FTPFile	FileRead, FileWrite, ?? (TCPPIInbound, TCPIPOutbound	May want to split into two events, one for reading and one for writing. Constrain to the common FTP port, unless the app is known by name to be an FTP client.	Like FileLeftThroughNetworkPort, look for interleaved reads and network events, or interleaved writes and network events.	Process
RemoteAccess	TCPIPIInbound, TCPIPOutbound, UDPIPInbound, UDPPOutbound, IPSECIInbound, IPSECOutbound	Do not incorporate FileRead events. Several ports may be used. Look for known image names of remote apps.		Process

FIG. 5C

9/10

TunnelOut	TCPIInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECIInbound, IPSECOutbound.	All events use same protocol. Only two processes used. Two different apps and four ports are used. One of the ports is remote. Event 1: The first app sends outbound from local port 1 to local port 2. Event 2: The second app (the tunneler) receives inbound from local port 1 to local port 2. Event 3: The tunneler also sends from local port 3 to remote port 4. Both events of the tunneler share the same thread (probably).	Login
TunnelIn	TCPIInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECIInbound, IPSECOutbound	All events use same protocol. Only two processes used. Two different apps and four ports are used. One of the ports is remote. Event 1: The first app (the tunneler) receives inbound from remote port 1 to local port 2. Event 2: The tunneler sends outbound from local port 2 to local port 3. Event 3: The second app also receives inbound from local port 3 to local port 4. Both events of the tunneler share the same thread (probably).	Login
TunnelInOut	TCPIInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECIInbound, IPSECOutbound	Multiple protocols may be used. More research needed. More than three ports are used.	Login
FileLeftThroughTunnel	FileRead, TunnelOut	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads involving a process that is participating in a TunnelOut event. If more than one file is read, the source destination will be a count of the files read.	Login?

FIG. 5D

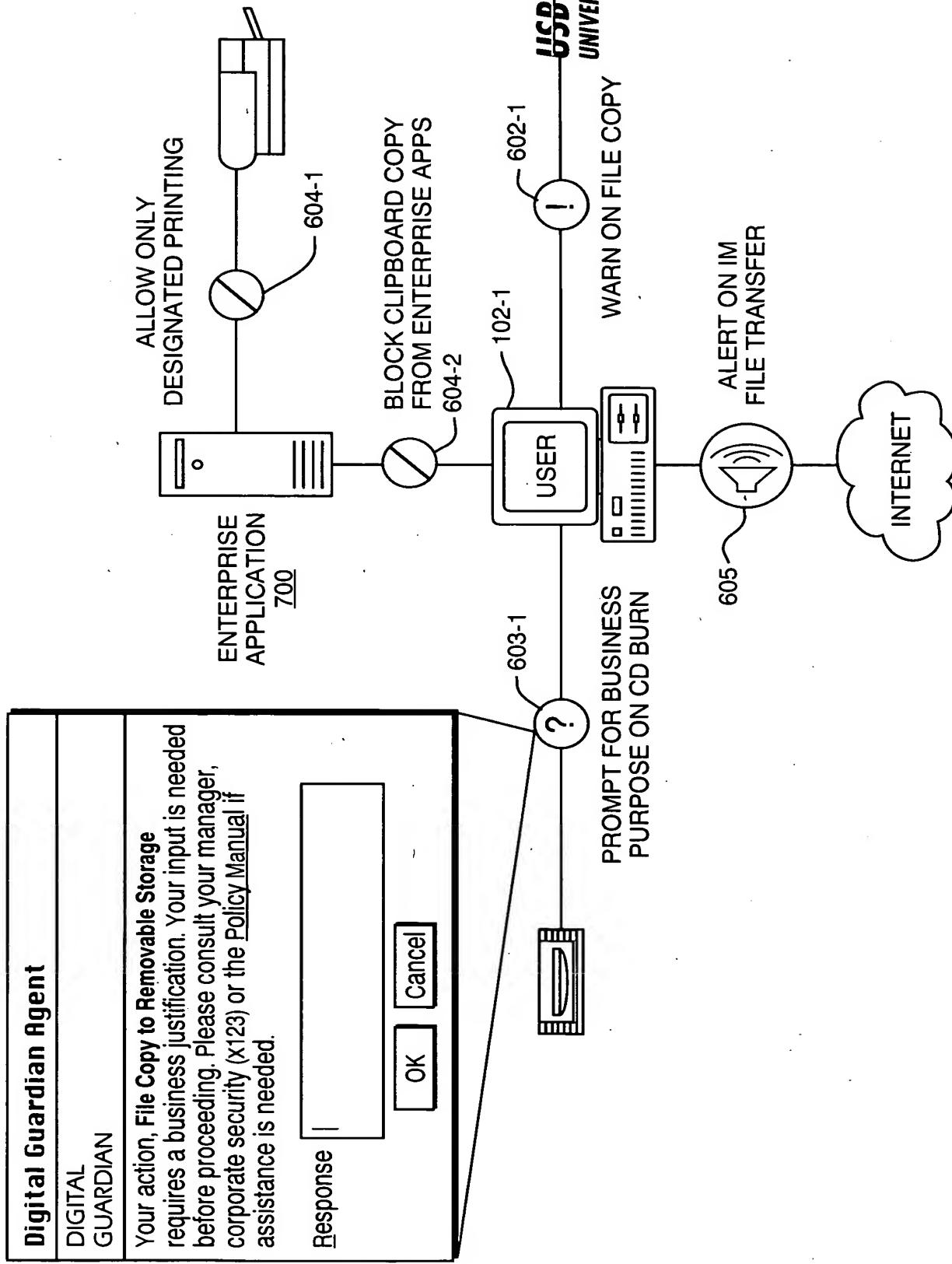


FIG. 6